Prime Numbers

Consider the decision problem \textsc{Prime}:

Given a number \(x\), is it prime?

This problem is in \textsc{co-NP}.

\[
\forall y (y < x \rightarrow (y = 1 \vee \neg \text{div}(y, x)))
\]

Note again, the algorithm that checks for all numbers up to \(\sqrt{n}\) whether any of them divides \(n\), is not polynomial, as \(\sqrt{n}\) is not polynomial in the size of the input string, which is \(\log n\).

Primality

In 2002, Agrawal, Kayal and Saxena showed that \textsc{Prime} is in \textsc{P}.

If \(a\) is co-prime to \(p\),

\[
(x - a)^p \equiv (x^p - a) \pmod{p}
\]

if, and only if, \(p\) is a prime.

Checking this equivalence would take too long. Instead, the equivalence is checked \textit{modulo} a polynomial \(x^r - 1\), for “suitable” \(r\).

The existence of suitable small \(r\) relies on deep results in number theory.

Factors

Consider the language \textsc{Factor}

\[
\{(x, k) \mid x\ has\ a\ factor\ y\ with\ 1 < y < k\}
\]

\textsc{Factor} \(\in\ \text{NP} \cap \text{co-NP}\)

\textit{Certificate of membership}—a factor of \(x\) less than \(k\).

\textit{Certificate of disqualification}—the prime factorisation of \(x\).
Optimisation

The Travelling Salesman Problem was originally conceived of as an optimisation problem to find a minimum cost tour.

We forced it into the mould of a decision problem – TSP – in order to fit it into our theory of NP-completeness.

Similar arguments can be made about the problems CLIQUE and IND.

Function Problems

Still, there is something interesting to be said for function problems arising from NP problems.

Suppose

\[ L = \{ x \mid \exists y R(x, y) \} \]

where \( R \) is a polynomially-balanced, polynomial time decidable relation.

A witness function for \( L \) is any function \( f \) such that:

- if \( x \in L \), then \( f(x) = y \) for some \( y \) such that \( R(x, y) \);
- \( f(x) = \text{“no”} \) otherwise.

The class FNP is the collection of all witness functions for languages in NP.

FNP and FP

A function which, for any given Boolean expression \( \phi \), gives a satisfying truth assignment if \( \phi \) is satisfiable, and returns “no” otherwise, is a witness function for SAT.

If any witness function for SAT is computable in polynomial time, then \( P = NP \).

If \( P = NP \), then for every language in NP, some witness function is computable in polynomial time, by a binary search algorithm.

\[ P = NP \text{ if, and only if, FNP = FP} \]

Under a suitable definition of reduction, the witness functions for SAT are FNP-complete.
**Factorisation**

The *factorisation* function maps a number \( n \) to its prime factorisation:

\[ 2^{k_1}3^{k_2} \cdots p_m^{k_m}. \]

This function is in \( \text{FNP} \).

The corresponding decision problem (for which it is a witness function) is trivial - it is the set of all numbers.

Still, it is not known whether this function can be computed in polynomial time.

**Cryptography**

Alice wishes to communicate with Bob without Eve eavesdropping.

**Private Key**

In a private key system, there are two secret keys

- \( e \) – the encryption key
- \( d \) – the decryption key

and two functions \( D \) and \( E \) such that:

for any \( x \),

\[ D(E(x, e), d) = x \]

For instance, taking \( d = e \) and both \( D \) and \( E \) as *exclusive or*, we have the *one time pad*:

\[ (x \oplus e) \oplus e = x \]

**One Time Pad**

The one time pad is provably secure, in that the only way Eve can decode a message is by knowing the key.

If the original message \( x \) and the encrypted message \( y \) are known, then so is the key:

\[ e = x \oplus y \]
Public Key

In public key cryptography, the encryption key $e$ is public, and the decryption key $d$ is private.

We still have,

$$D(E(x, e), d) = x$$

If $E$ is polynomial time computable (and it must be if communication is not to be painfully slow), then the function that takes $y = E(x, e)$ to $x$ (without knowing $d$), must be in $\text{FNP}$.

Thus, public key cryptography is not provably secure in the way that the one time pad is. It relies on the existence of functions in $\text{FNP} - \text{FP}$.